



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

MAY 04 2007

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
ASSISTANT SECRETARIES OF DEFENSE  
GENERAL COUNSEL OF THE DEPARTMENT OF  
DEFENSE  
INSPECTOR GENERAL OF THE DEPARTMENT OF  
DEFENSE  
COMMANDERS OF THE COMBATANT COMMANDS  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD Information Sharing Strategy

In response to Quadrennial Defense Review (QDR) direction, the DoD CIO, USD(P), USD(I) and the CJCS have developed a DoD Information Sharing Strategy. The Strategy provides a common vision to synchronize initiatives to share information among DoD components, all levels of US government, international coalition partners, and the private sector and also supports the national strategy on information sharing. Through execution of this Strategy the Department aims to achieve improved unity of effort, quality and speed of decision-making, increased adaptability of forces, improved situational awareness, and greater precision in mission planning and execution.

To execute this Strategy, an action oriented implementation plan and governance process is required. Progress in these areas is as follows:

- An Information Sharing Senior Steering Group (ISSSG) has been established consisting of the DoD CIO, USD (P), USD(I) and CJCS to serve as the focal point for guidance, direction and oversight of DoD information sharing initiatives. As our governance process is developed, the membership will be expanded to include a broader representation of our information sharing community.



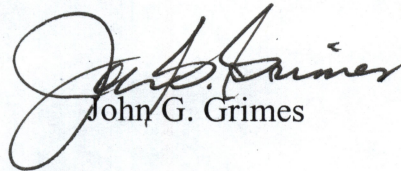
Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>04 MAY 2007</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2007 to 00-00-2007</b>	
4. TITLE AND SUBTITLE <b>DoD Information Sharing Strategy</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Department of Defense,6000 Defense Pentagon,Washington,DC,20301-6000</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>24</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			



- A team and high-level approach have been established to develop an Implementation Plan and a DoD Directive. The Plan will define near-term actions and milestones necessary to execute the Strategy. The Directive will codify policies, roles and responsibilities on information sharing within the DoD.

The Plan and Directive will require additional organizational participation and access to subject matter experts; therefore, request each addressee provide a Point of Contact within 15 days to support the development of the Plan and Directive.

The point of contact for this effort is Mr. Paul D. Grant. He can be reached at Paul.Grant@osd.mil, or 703-607-0383.



John G. Grimes

Attachment:  
As stated

# **Department of Defense Information Sharing Strategy**



**O4 May 2007**

**Prepared by:  
Department of Defense  
Information Sharing Executive  
Office of the Chief Information Officer**

## EXECUTIVE SUMMARY

This Information Sharing Strategy provides a common vision to synchronize information sharing initiatives and investments throughout the Department. Sharing of information is an increasingly important element of Departmental mission success. It is imperative to effectively exchange information among components, Federal agencies, coalition partners, foreign governments and international organizations as a critical element of our efforts to defend the nation and execute national strategy. Through this Strategy, the Department will achieve improved unity of effort, a reduction in decision time, increased adaptability of forces, improved situational awareness, and greater precision in mission planning and execution.

The Department of Defense (DoD) requires innovations to enhance information sharing across the Department and with external partners. The evolving United States national security environment necessitates an improvement to the Department's ability to effectively and securely share information. Multiple national and departmental strategies affect information flow and accessibility, limiting the ability to leverage information as a strategic asset in achieving the Department's mission. Further, current events have diverse and global-reaching impacts, drawing the DoD into operations with diverse and unanticipated partners.

The DoD Information Sharing Strategy establishes the vision and goals for information sharing, while paving the way for a more detailed initiative to document the implementing actions necessary to achieve these goals and realize the vision.

Improving the Department's ability to share information helps the DoD realize the power of information as a strategic asset. Benefits include, but are not limited to: (1) Achieving unity of effort across mission and coalition operations, (2) Improving the speed and execution of decisions, (3) Achieving rapid adaptability across mission and coalition operations, and (4) Improving the ability to anticipate events and resource needs, providing an initial situational advantage and setting the conditions for success.

The Department of Defense (DoD) Information Sharing Strategy provides the common vision, goals and approaches that guide the many information sharing initiatives and investments for all DoD.

Information sharing is defined as, “**Making information available to participants (people, processes, or systems).**” Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant. This DoD Strategy establishes the vision for the future:

**Deliver the power of information to ensure mission success**  
**through an agile enterprise with freedom of maneuverability across the information environment.**

The vision describes a future state where transparent, open, agile, timely, and relevant information sharing occurs to promote freedom of maneuverability across a trusted information environment. To achieve the vision, this Strategy describes four goals that form the necessary environment across the DoD. These goals are: (1) promote, encourage, and incentivize sharing; (2) achieve an extended enterprise; (3) strengthen agility in order to accommodate unanticipated partners and events; and (4) ensure trust across organizations.

The Information Sharing Strategy guides the Department's sharing of information within the DoD and with Federal, state, local, tribal, coalition partners, foreign governments and security forces, international organizations, non-governmental organizations, and the private sector, hereafter referred to as external partners. The Strategy represents the first step in a comprehensive initiative to assess and modify as needed existing policies, business processes, budget allocations, and cultural perspectives.

The focus on improving information sharing across the U.S. federal government is reflected in White House guidance, such as Executive Order 13388 "Further Strengthening the Sharing of Terrorism Information to Protect Americans", legislation, such as the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, and international cooperatives, such as the Multi-National Information Sharing (MNIS) initiative. Numerous independent mission or functional area specific initiatives address aspects of information sharing from intelligence and counter-terrorism, multinational, and stability operations, to humanitarian assistance and disaster relief. ***These strategies and efforts must be synchronized in order to achieve unity of effort as well as economic and operational efficiencies.***

The DoD Information Sharing Strategy establishes five touchstones of information sharing: Culture, Policy, Governance, Economics and Resources, and Technology and Infrastructure. Each stakeholder community shall improve these five areas to realize the overall goals of this Strategy.

DoD shall develop an Information Sharing Strategic Implementation Plan as a companion document. This Plan will provide integrated guidance to synchronize the many information sharing activities, initiatives and investments supported by the DoD, including both internally and externally sponsored efforts. The Plan will expand the five implementation considerations identified in this Strategy and provide descriptions of the specific actions, roles, responsibilities, milestones and metrics.

Every individual and organization in the Department of Defense plays an important role in improving information sharing. Successful accomplishment of this Strategy will result in efficiencies in operations, enhanced and shared situational awareness, and – ultimately – mission success. This strategy requires your involvement, assistance, and commitment.



John G. Grimes  
DoD CIO



## TABLE OF CONTENTS

Purpose.....	2
Vision.....	3
Information Sharing Landscape .....	3
Goals .....	5
Approaches to Achieve the Goals.....	6
Implementation Considerations .....	10
Culture.....	10
Policy .....	11
Governance .....	12
Economics and Resources.....	12
Technology and Infrastructure .....	13
Strategic Communications and Outreach.....	14
Appendix A. Glossary.....	16
Appendix B. Acronyms .....	18



## Purpose

The Department of Defense (DoD) Information Sharing Strategy provides the common vision, goals and approaches that guide the many information sharing initiatives and investments for the Department. This Strategy fulfills the imperative identified in the Quadrennial Defense Review (QDR). The Information Sharing Strategy guides the Department's exchange of information within the DoD and with Federal, state, local, tribal, coalition partners, foreign governments and security forces, international organizations, non-governmental organizations, and the private sector, hereafter referred to as external partners. This Strategy describes the information sharing approach for the Office of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Military Departments, the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the DoD. It guides the information sharing activities and operations among these DoD entities and with external partners. The Strategy establishes the Departmental foundation for strategic implementation planning.

DoD shall develop an Information Sharing Strategic Implementation Plan as a companion document. This Plan provides integrated guidance to synchronize the many information sharing activities, initiatives and investments supported by the DoD, including both internally and externally sponsored efforts. The Plan expands the five implementation considerations identified in this Strategy and provides descriptions of the specific actions, roles, responsibilities, milestones, metrics, and priorities.

“Develop an information-sharing strategy to guide operations with Federal, state, local, and coalition partners.”  
- QDR February 2006

Effective information sharing enables the DoD to achieve dynamic situational awareness and enhance decision making to promote unity of effort across the Department and with external partners. To accomplish these outcomes, this Strategy addresses the necessary changes to information mobility and the associated alignment of incentives, policies, processes, and systems. Additionally, this Strategy identifies the critical cultural shift required to support collaboration and improved knowledge sharing.

The DoD intends to continue operating in the evolving federated approach for information sharing. Therefore this Strategy assumes that external partners' sharing capabilities and philosophies will not necessarily conform to the DoD environment and culture, and that in the federated environment, autonomous enterprises will reach mutual agreement about participation in information sharing and the appropriate rules and standards of conduct.

## Vision

The vision describes the desired future state for DoD Information Sharing. It describes something that does not exist today, and it intentionally states “what” the future state includes, rather than “how” the Department arrives at such a state. The vision for information sharing for the DoD is:

**“Transforming to a network-centric force requires fundamental changes in process, policy, and culture.”**

National Defense Strategy, March 2005

**Deliver the power of information to ensure mission success through an agile enterprise with freedom of maneuverability across the information environment.**

The vision above and the strategy articulated in this document enhance the Department’s position on information sharing by aligning the actions, initiatives, and behaviors of all involved. The vision describes a future state where transparent, open, agile, timely, relevant, and trusted information sharing occurs to promote freedom of maneuverability across the information environment. Successful accomplishment of this vision will result in efficiencies in operations, enhanced and shared situational awareness, and – ultimately – mission success.

## Information Sharing Landscape

Improving information sharing constitutes a cornerstone of our national priorities. The mandates that enable and support this goal reside at the highest levels of authority - from Public Law to Presidential Executive Orders, National Strategies, and the DoD QDR. The evolving United States national security environment provides a context that is ripe for advancing innovations to enhance the value of information across the DoD and other agencies. Within this context, the DoD is pursuing opportunities to exploit information dominance against our adversaries and support effective, unified actions with our external partners.

*“The federal government is the largest purchaser of information technology in the world by far. One would think we could share information by now. But Katrina again proved we cannot.”*

Executive Summary of Findings: Page 1, Congressional Reports: H. Rpt. 109-377 - A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina

As a result of the broad scope and multiple facets within the information environment, the definition of information sharing has taken on several variations. For purposes of this Strategy, information sharing is defined as, **“Making information available to participants (people, processes, or systems).”** Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant.

The means by which information is shared in the information sharing landscape is vast, ranging from face-to-face interactions to real-time voice communications, to the latest

messaging and data technologies that pass information across trusted networks. The Department must have the ability to transfer information to and obtain information from external partners overcoming situations where these partners may have disparate processes and capabilities and whose role and nature may not be known prior to an event. The DoD will share sensitive information currently protected by statute with authorized users, while maintaining an awareness of where and how this information is used.

Current events have diverse and global-reaching impacts, drawing the DoD into operational scenarios with varied partners. The DoD cannot always anticipate the events of tomorrow - solutions must transcend today's scenarios and provide the DoD the ability to accommodate dynamically changing coalitions, external partners, and information sharing requirements. The multiple, ongoing efforts in the pursuit of information sharing demonstrate that classified/national security-related information is one of many national priorities for information sharing.

Numerous independent mission or functional area specific initiatives address aspects of information sharing from intelligence and counter-terrorism, multinational, and stability operations, to humanitarian assistance and disaster relief. These individual efforts, while yielding benefits, are narrowly focused with no coordination or overarching guidance. This problem-specific approach continues to result in gaps, disparate solutions, and redundant efforts. This leaves significant issues associated with normalization of standards, cost inefficiency, risk management, trust mechanisms, and agreed upon rules for information categorization, classification and sharing.

The DoD acknowledges the value of information sharing cannot be fully achieved with multiple independent initiatives. The QDR directs the Department to: "Improve the Department's information sharing with other agencies and with international allies and external partners by developing information protection policies and exploiting the latest commercial technologies...to improve information sharing and information assurance, and extend it across a multitude of domains, ranging from intelligence to personnel systems."

***"We must recognize that we are woefully incapable of storing, moving, and accessing information - especially in times of crisis."***

Executive Summary of Findings: Page 1,  
Congressional Reports: H. Rpt. 109-377 - A  
Failure of Initiative: Final Report of the  
Select Bipartisan Committee to Investigate  
the Preparation for and Response to  
Hurricane Katrina

The DoD recognizes and shall leverage national and departmental strategies and shall promulgate policy and guidance to promote and embrace information flow and accessibility within the Department and with other external partners. Comprehensive, effective response that maximizes freedom of maneuverability requires unity of effort, consistent guidance, and efficient ties into the budget and resource allocation process. This Strategy leads the shift from situational-based initiatives to a comprehensive unity of effort establishing supremacy in the information environment.

## Goals

The goals describe the interrelated concepts needed to move the DoD from the current state of information sharing to the vision. The information sharing goals form an environment across the DoD that will:

### 1. Promote, encourage, and incentivize sharing.

Successful information sharing necessitates a mindset where information is continually shared as a normal course of work. It begins when organizational leaders set the example and demonstrate their commitment by advocating for information sharing, and will be realized when the dissemination of information is supported at all organizational levels. Leaders shall align individuals to the common information sharing vision and encourage the adoption of the new mindset and culture. A common set of unifying approaches to DoD Information Sharing will be developed, requirements validated, and individuals trained on the proper tools, techniques and procedures so that this common set of information sharing practices is used at all levels throughout the Department.

### 2. Achieve an extended enterprise.

The extended enterprise refers to all internal and external participants required to ensure mission success. This facilitates collaborative and coordinated decision making, shared situational awareness and improved knowledge at every level. The extended enterprise requires the alignment of plans, processes, and systems across organizational and functional boundaries.

For Katrina, the **extended enterprise** included DoD (active and reserve), National Guard, DHS, FEMA, US Coast Guard, state and local governments, first responders, NGOs and SPCA.

### 3. Strengthen agility, in order to accommodate unanticipated partners and events.

Though it is important that the DoD continue to proactively plan for information sharing with anticipated partners and events, it is also critical to prepare for unanticipated partners and events. To accomplish information sharing in diverse and disadvantaged situations, the DoD shall enact and implement adaptive policies, guidance, practices, protections, and technologies.

### 4. Ensure trust across organizations.

A cornerstone of information sharing is trust - trust in the partner organizations including, but not limited to, their policies, procedures, systems, networks, and data. The DoD shall develop methods to promote and establish trust. These methods will take into account and remain agile to accommodate differing levels of trust based on the environment, situation, and extended enterprise.

## Approaches to Achieve the Goals

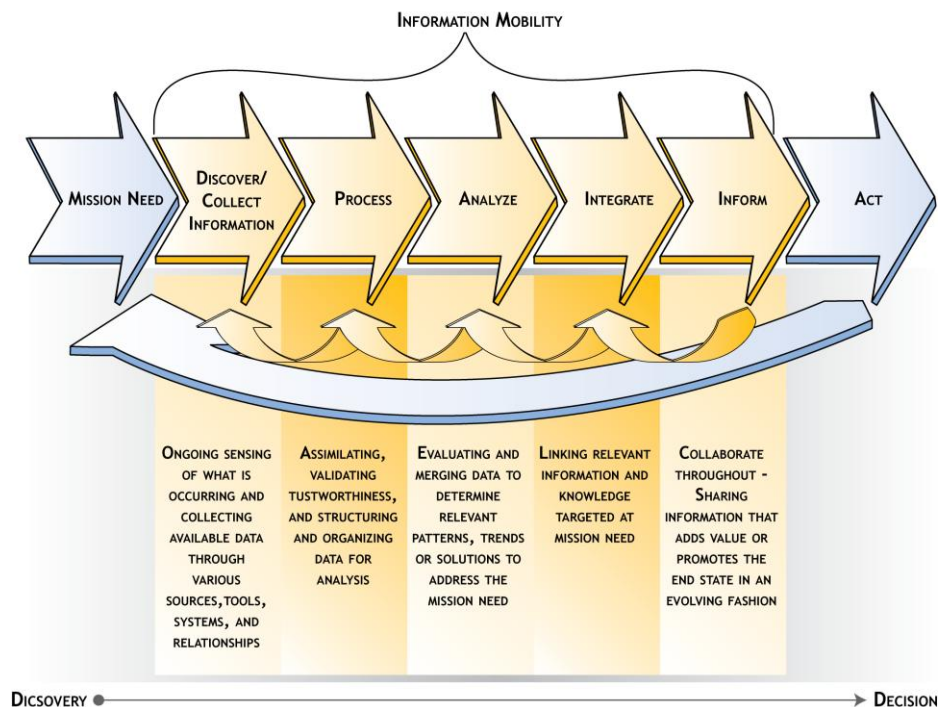
The information sharing goals will be accomplished through implementation of the following approaches.

### 1. Recognize and leverage the Information Sharing Value Chain.

The Information Sharing Value Chain articulates the “opportunity” of information sharing to support informed decision making, shared situational awareness and improve knowledge at every level of the DoD. The risks encountered at each step of the information sharing value chain must be managed to mitigate negative consequences.

Throughout history, the supply of and demand for information triggers the inter-related processes of information collection, processing, analysis, and integration to make informed decisions, increase situational awareness, or improve and manage knowledge. Regardless of the mission domain, community or organization’s unique processes for managing information, the universal Information Sharing Value Chain (as shown in Figure 1) remains the same – to discover and collect information and continuously add value at each stage to best inform a decision maker. In Figure 1, the information sharing activities are described by the “Discovery to Decision” continuum. This continuum provides the perspective of continual collaboration and enhancement of data to create relevant and actionable knowledge.

Figure 1: Information Sharing Value Chain





The strategic shift (opportunity) for the Department's information sharing is to create the governance, policy, technology, culture and economics that promote all aspects of the Information Sharing Value Chain and facilitate the access, sharing and integration of information such that the DoD has freedom of maneuverability.

*"Many of the problems we have identified can be categorized as 'information gaps' - or at least problems with information-related implications or failures to act decisively because information was sketchy at best."*

Executive Summary of Findings: Page 1,  
Congressional Reports: H. Rpt. 109-377 - A Failure  
of Initiative: Final Report of the Select Bipartisan  
Committee to Investigate the Preparation for and  
Response to Hurricane Katrina

## 2. Forge information mobility.

Information mobility is the dynamic availability of information which is promoted by the business rules, information systems, architectures, standards, and guidance/policy to address the needs of both planned and unanticipated information sharing partners and events. Information mobility provides the foundation for shared and user-defined situational awareness. Trusted information must be made visible, accessible, and understandable to any authorized user in DoD or to external partners except where limited by law or policy.

Information mobility is both the foundation and core of the DoD Information Sharing capability. There are *five* elements of information mobility, as described by the following functional areas:

**Technology** – enables the flow, management and processing of information. Technology includes architecture, core enterprise services, and information communications and technology infrastructure. Technology must support information mobility by requiring trusted information to be visible, accessible, and understandable to any authorized user in DoD or to external partners except where limited by law or policy.

**Workforce Information Sharing Competence** – the workforce's ability to share information across the enterprise. Workforce competence will be promoted through leadership examples, shifts in cultural norms, and training on tactics, techniques and procedures.

**Social Networks** – the ability to form and join social networks and communities of practice. Trust relationships often begin with individual interactions that reinforce a shared mental model of the decision environment. Opportunities and norms to establish these networks, build trust in, and accommodate the individual's operating practices will be developed through the federated information sharing community approach.

**Policies** – that enable information mobility across operational domains, clarifies roles and responsibilities, defines relationships, harmonizes rules and procedures, and creates a risk managed environment that protects privacy and personal liberties. Spans entire information life cycle process from discovery to disposition.

**Security** – that promotes information protection and sharing with assurance and trust of information availability, integrity, authentication, confidentiality, and non-repudiation.

### 3. Make information a force multiplier through sharing.

Information as a force multiplier refers to exploiting relative information advantages against our adversaries and to support effective, unified disaster response. Sharing is inherent in information becoming a force multiplier and results in increased operational effectiveness.

The following factors are challenges that must be addressed to enable information sharing to serve as a force multiplier:

**Volume** - The amount of data that exists that could support the specific mission need or event. As information sharing improves, the volume of data available to analyze for decision making will continue to grow.

**Veracity** - The ability to create relevance and de-conflict potentially conflicting data received from a number of sources. While analysts and decision-makers may receive more information, more quickly, and from more directions, its accuracy, consistency, authority, currency and completeness must be validated.

**Velocity** - The timeliness of information required as compared to the ability to obtain, transfer, and share information. Analysts and decision makers can receive a multitude of information from a variety of sources, in real- or near-real-time.

**Vector** - Information sharing is increasingly multidirectional and crosses domains and boundaries (e.g., mission, functional, organizational, security, classification).

### 4. Promote a federated Information Sharing Community/Environment.

Governance, policy and cultural considerations establish the required multi-lateral relationships working in a regulated, risk management environment that ensures information security, privacy, and trust. The federated approach establishes and maintains a trusted community of information sharing that promotes collaboration, leverages the information integrators in the community and reduces the “seams” between organizations, domains and functions.

DoD operates with a federated approach to information sharing with external partners. This approach establishes the relationship between legally autonomous entities and provides a binding framework for information sharing and collaboration. Federated information sharing includes trust mechanisms, standards, procedures and audit regimes to establish and maintain trust and compliance with the federation agreements.

*“Organizations that had worked together in the past and had brought their information systems into alignment were able to respond much more quickly to the disaster.”*

“Lessons from KatrinaHealth,” a Markle Foundation Report, 13 June 2006, detailing the effort to coordinate and share individual health records with physicians treating dispersed evacuees.

**5. Address the economic reality of information sharing.**

Create guidance and incentives within the budgeting and resource allocation process to encourage organizations to share information that promotes informed decision making, improves situational awareness, establishes economies of knowledge, and creates unity of effort.

Orchestrating funding and resource investments is critical for the successful implementation of information sharing and achievement of unity of effort. Existing initiatives, resources and evolving requirements must be integrated to efficiently use scarce resources. The requirements, acquisition and Planning, Programming, and Budgeting System (PPBS) processes must be synchronized to efficiently provide funding and resources. A risk management approach will determine resource allocation and investment. Measures of effectiveness will determine return on investment and the effectiveness of the DoD information sharing initiative.

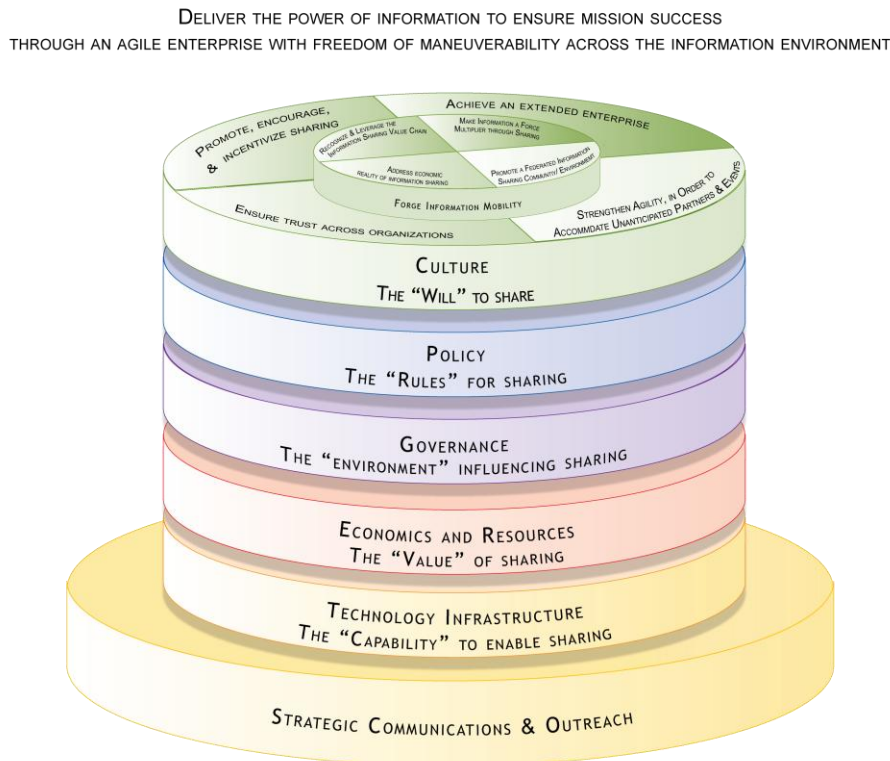
## Implementation Considerations

This Strategy requires the development and execution of the Information Sharing Strategic Implementation Plan. Implementation planning and execution will be widespread and occur at all levels. Success will be a unified and coordinated set of initiatives, spanning from Department leadership to system owners and operators, to the warfighter.

The future cross-cutting Information Sharing Implementation Plan will consider five key touchstones: culture, policy, governance, economics and resources, and technology and infrastructure. (as shown in Figure 2).

This Strategy provides the umbrella under which the implementation of current and future information sharing initiatives will align.

Figure 2: Information Sharing Implementation Touchstones



### Culture

Successful information sharing requires a major cultural shift across the DoD. There is an established mindset of information "ownership". The new mindset must be one of information "stewardship". The best technology, processes, and policies will not make this successful if the people do not embrace the new cultural norms.

#### The Need for Organizational Flexibility.

"...The protocols in place on 9/11 for the FAA and NORAD to respond to a hijacking presumed that...there would be time to address the problem through the appropriate FAA and NORAD chains of command."

The 911 Commission Report, p.18

To facilitate this shift, organizational leaders must support this cultural change, set the example, educate their people, and offer incentives for, and enforcement of information sharing and stewardship.

The organizational approach and philosophy to adopt a sharing posture will be driven through shared missions and the ability/flexibility to ‘realign’ and adapt to changing circumstances. Specific implementation activities will include, but are not limited to:

- Influence all training curriculums from basic training to senior service schools.
- Train on tactics, techniques, and procedures (TTPs) that clearly outline information sharing approach and implementation plans.
- Require each information sharing program or initiative to address the cultural considerations in implementation planning.
- Establish a trusted risk management environment (and mindset).
- Foster an environment to share information.
  - Recognize leaders who promote an information sharing environment.
  - Offer incentives to embrace information sharing and stewardship.
  - Encourage participation in Communities of Interest.

## **Policy**

Clear, concise and comprehensive guidance is necessary to implement this Information Sharing Strategy. Laws, policies, regulations, and business rules must be evaluated and adjusted, as required, to facilitate the flow of information across the federated information sharing community, including all external partners. Policies must be consistent and harmonized at multiple levels, including national and international laws and regulations that affect all federal departments and agencies; individual agency guidance for information sharing between and within agencies; policies guiding Federal, state, local and tribal relationships; and regulations affecting sharing and protection of information between government agencies and the private sector. Precise guidance will result in common methods and approaches, and promote both security and unity of effort.

Specific implementation activities will include, but are not limited to:

- Assess existing policy and guidance to address gaps and differences.
- Reconcile diverse rules for information sharing among partners.
- Establish and promote a federated approach with all partners.
  - Establish trustworthiness – people, technology, data, and processes.
- Develop and align policy to improve information mobility.

**Flexible Policy Execution.** *The Department of Health and Human Services (DHHS) Office for Civil Rights (which oversees HIPAA) issued a special bulletin clarifying that, considering the emergency circumstances, organizations that did not comply with the usual business associate requirements would not be penalized as long as they showed “good faith efforts” to protect the privacy of health information “and to appropriately execute the agreements required by the Privacy Rule as soon as practicable.”* “Lessons from KatrinaHealth,” a Markle Foundation Report, 13 June 2006



- Establish consistent rules for sharing information.
  - Establish simple and consistent rules for identifying, handling, and protecting controlled information.
- Promote sharing while preserving individual privacy protections and/or civil liberties.
- Influence planning and programming guidance.

## **Governance**

A comprehensive, widely understood governance framework is critical for creating and sustaining a federated information sharing community of organizations and individuals aligned to the information sharing vision and agreed upon rule sets and processes. The governance framework must articulate the accountability and authority; promote standards and guidelines; ensure a consistent well-defined approach, processes and procedures; adjudicate disconnects; establish legal and policy enforcement; and use performance measures to ensure progress towards achieving the information sharing goals.

The DoD's information sharing governance framework leverages existing structures and mechanisms, as well as employs new ones as needed. The Department uses a federated approach that establishes the relationship between legally autonomous entities focused on a common result. This provides a binding framework for information sharing and collaboration, acknowledges interdependencies, and fosters outreach, communication and coordination. A federated information sharing community synchronizes the many initiatives and investments through visibility and alignment.

*"In addition to avoiding centralization where possible, KatrinaHealth was structured in such a way as to prohibit access to aggregate data. Authorized physicians and pharmacists had the ability to dispatch a query for one patient at a time only... and their query could not be successfully submitted unless they were authorized and had obtained specific information about the patient."*

"Lessons from KatrinaHealth," a Markle Foundation Report, 13 June 2006

Specific implementation activities will include, but are not limited to:

- Assign responsibilities for the authority, oversight, coordination, and integration of information sharing across the DoD and with external partners.
- Implement processes to:
  - Promote standards and guidelines,
  - Ensure a consistent well-defined approach,
  - Adjudicate disconnects,
  - Establish legal and policy enforcement, and
  - Measure performance.
- Align current information sharing initiatives and programs.

## **Economics and Resources**

The DoD shall tie information sharing to the Department's fiscal dimension. The QDR specifically directs that the Department will "...reach investment decisions through collaboration among the joint warfighter, acquisition and resource communities...begin

to break out its budget according to joint capability areas...manage the budget allocation process with accountability ... (and) establish 'Capital Accounts' for Major Acquisition Programs.”

In order to comply with the QDR and to maximize capabilities, the Department will strategically prioritize planning and Program Objective Memorandum submissions and purposefully guide Program Evaluation Guidance deliberations. Through portfolio management, a coordinated, integrated enterprise will make DoD Information Sharing not only more timely, but also more efficient and cost effective for the government. The up-front investment in the vertical and horizontal alignment of plans, processes, and systems for information sharing across organizational and functional boundaries will facilitate collaboration and informed decision making, and will ultimately result in a significant return-on-investment for the DoD.

*"DoD lacked an information sharing protocol that would have enhanced joint situational awareness and communications between all military components."*

Executive Summary of Findings: Page 4, Congressional Reports: H. Rpt. 109-377 - A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina

To this end, the DoD will create guidance and incentives within the budgeting and resource allocation process to encourage organizations to share information that promotes informed decision making, improves situational awareness, establishes economies of knowledge, and reduces duplication of effort. This is always a priority, but will be even more critical as the Department enters an era of potentially diminishing resources.

Specific implementation activities will include, but are not limited to:

- Incorporate information sharing objectives into the requirements, acquisition, planning, and budgeting processes (e.g., JCIDS, PPBS, acquisition process).
- Establish guidance and priorities within the budgeting and resource allocation process.
- Leverage synergy of combined investments with external partners

## ***Technology and Infrastructure***

Enabling information sharing through the use and practice of current technology and the exploitation of potential future technology allows for improvements to the assured flow, management, and processing of information. The DoD will leverage the many investments it has made, and will continue to make, within the net-centric and the information technology (IT) environment. The DoD will work with external partners who have highly developed technology support for information sharing while maintaining capabilities to work with external partners who have limited or no technology support for information sharing.

The DoD must keep in mind that technology alone will not solve the information sharing gap. While leveraging available technologies to the fullest extent, the DoD will continue to advance itself and its external partners in the areas of information delivery,

collaboration, and information and knowledge management. The DoD will ensure continued investment, business process advancement, overarching technology standards, and the promotion of a broader information sharing culture among people and organizations. These efforts will allow the DoD to realize the full benefits that technology will provide as an enabler within the DoD community and for our partners.

Emerging technologies offer varying levels of increased capability for information sharing. The emphasis for DoD will be on procuring technology that is standards-based and conformant to DoD architectures. Technology procurements to support information sharing must be guided by the tenets of interoperability, accessibility, ease of use, and compliance with security directives.

Specific implementation activities will include, but are not limited to:

- Comply with the DoD Enterprise Architecture and Federal Enterprise Architecture guidance.
- Implement Federally compliant strong identity and access control.
  - Conform to the Federal Identity Management Federation standards.
  - Advocate technically equivalent solutions with other external partners.
- Implement existing DoD and Federal technology strategies.
- Apply technology to improve information mobility by requiring trusted information to be visible, accessible, and understandable to any authorized user in DoD or to external partners except where limited by law or policy.
- Participate in developing, promoting, and enabling use of standards by partners.

## Strategic Communications and Outreach

Transforming the DoD to an organization with an information sharing mindset is a challenging effort. The DoD must address and change deeply rooted paradigms of “how things have always been done.” Involving DoD stakeholders through communications and outreach is crucial to gaining the buy-in and participation that is needed to successfully foster information sharing. Leaders, in particular, will play a key role in defining this change and in building support both across the Department and with external partners.

The Department-wide communication and outreach initiative is an ongoing effort to ensure that this Information Sharing Strategy and future Implementation Plans are properly promulgated, commonly understood and that all interested parties, programs, and initiatives can recognize their role in the information sharing vision. Communication planning involves the development of messages that are used to describe key aspects of the Information Sharing Strategy and Implementation Plans. This communication effort has begun and will continue to evolve. The initial messages that the DoD has developed for communication include:

- *The Information Sharing Strategy shifts information sharing from situational-based initiatives to a comprehensive unity of effort..*

- *The intent of the Information Sharing Strategy is to have single, integrated guidance that synchronizes information sharing initiatives and investments to achieve the vision. This guidance and associated processes and tools will give the DoD the flexibility to share information with planned and unanticipated partners across planned and unanticipated events.*

The messages are matched to the appropriate stakeholders to ensure that groups receive what is most important to their interests. The intent is to build lasting commitment that will propel DoD Information Sharing toward the Department's vision.

As part of the outreach activities, the DoD will assist in the establishment of social networks and Communities of Practice to inform, involve, and align stakeholders in the undertaking of information sharing initiatives. In addition, the Department will seek opportunities to reach out to partner organizations that may benefit from this information sharing initiative. It is through these outreach activities that the DoD and its external partners will learn and implement best practices in information sharing. The communications and outreach initiative must be a strategic, Department-wide effort to inform, involve, and mobilize the DoD and its partners toward the information sharing vision.

**Strategic Communications and Outreach.**

*"In July 1995, Attorney General Janet Reno issued formal procedures aimed at managing information sharing between Justice Department prosecutors and the FBI...These procedures were almost immediately misunderstood and misapplied. As a result, there was far less information sharing and coordination between the FBI and the Criminal Division in practice than was allowed under the department's procedures."*

The 911 Commission Report," p. 79

## Appendix A. Glossary

**Collaboration** – pattern of interaction where two or more parties are working together toward a common purpose.

**Data** – Representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by humans or automatic means. Any representation such as characters or analog quantities to which meaning is or might be assigned. (*source: Joint Publication 1-02 of 12 April 2001 as amended through 09 Nov 2006*)

**Domains** - A sphere of activity, concern, or function (*source: The American Heritage® Dictionary*).

**Enterprise Integration** – The vertical and horizontal alignment of plans, business processes, and information systems across organizational and functional boundaries to provide competitive advantage.

**Federation** –

1. Autonomous organizations operating under a common rule set to a common purpose.
2. Legally-binding framework to establish and maintain trust among autonomous organizations.

**Information** –

1. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms (*source: DoD Directive 8000.1*).
2. Facts, data, or instructions in any medium or form.
3. The meaning that a human assigns to data by means of the known conventions used in their representation (*source: DoD Dictionary <http://www.dtic.mil/doctrine/jel/doddict/>*).

**Information Mobility** - The dynamic availability of information. Information mobility is aided or impeded by culture, policy, governance, economics and resources and technology and infrastructure.

**Information Sharing** - Making information available to participants (people, processes, or systems). Information sharing includes the cultural, managerial, and technical behaviors by which one participant leverages information held or created by another participant.

**Networks** – A complex, interconnected group or system (*source: The American Heritage® Dictionary*). These networks include social, information technology, and communication networks.



Partner – an entity that takes part in an information sharing activity with DoD

**Risk Management** - The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits (*source: DoD Dictionary <http://www.dtic.mil/doctrine/jel/doddict/>*).

**Stakeholder** – a DoD entity with a direct interest, involvement, and investment in DoD information sharing.

## **Appendix B. Acronyms**

DHS – Department of Homeland Security

DoD – Department of Defense

FEMA – Federal Emergency Management Agency

JCIDS – Joint Capabilities Integration and Development System

MNIS – Multi-National Information Sharing

NGO – Non-Governmental Organization

PPBS – Planning, Programming, and Budgeting System

QDR – Quadrennial Defense Review

SPCA – Society for the Prevention of Cruelty to Animals

TTP – Tactics, Techniques, and Procedures